IN THE CLAIMS

1. (currently amended) A method of creating a digital certificate for a user comprising:

generating a user private key and a user public key;

obtaining ~~deriving~~ a ~~first data~~ set of attributes containing data pertaining to the user and useful to an issuing party issuing the digital certificate;

~~associating a user public key with the first data set thereby creating a second data set, the user public key and a corresponding user private key both generated and authenticated before the creation of a digital certificate by the issuing party;~~

encrypting ~~the second data set~~ the combination of said user public key and said set of attributes using an issuer private key to create an encrypted data set;

creating a digital certificate containing the user public key, the ~~first data~~ set of attributes, and the encrypted ~~second~~ data set, the digital certificate including ~~being identifiable by~~ an issuing-party identifier; and

storing the digital certificate at a user-allotted memory segment of a certificate library server; ~~, in which one or more digital certificates for the user can be stored at the user-allotted memory segment.~~

storing said user private key and an address of said certificate library server on a chip card of said user, whereby said digital certificate is stored remote from said chip card.

2. (currently amended) A method as recited in claim 1 further including ~~associating~~ creating a certificate chain using ~~with~~ the digital certificate, the certificate chain being stored in the user-allotted memory segment of a certificate library server and having a trusted root, the trusted root being different from other trusted roots stored at the user-allotted memory segment.

3. (cancelled)

4. (cancelled)

5. (currently amended) A method as recited in claim 1 further including accessing the digital certificate in the certificate library server using the issuing-party identifier, whereby said issuing party accesses said digital certificate to authenticate said user.

6. (cancelled)

7. (currently amended) A method as recited in claim 1 further including determining which party signed the encrypted ~~second~~ data set by retrieving a public key from another digital certificate of said certificate library server.

8. (currently amended) A method as recited in claim 7 further including decrypting the encrypted ~~second~~ data set and comparing the decrypted ~~second~~ data set with said user public key and said set of attributes ~~the second data set~~.

9. (currently amended) A method as recited in claim 1 further ~~including~~ including:

presenting an authentication challenge ~~a text string~~ to said user's chip card to be signed by ~~the corresponding~~ said user private key;

receiving an encrypted response from said chip card; and

decrypting said encrypted response using said user public key, whereby said chip card is authenticated.

10. (cancelled)

11. (cancelled)

12. (currently amended) A method as recited in claim 1 wherein the certificate library server is a Lightweight Directory Access Protocol (LDAP) server.

13. (currently amended) A method of authenticating a user's relationship with a registration authority by ~~user~~ presenting a chip card to a reliant party ~~an entity~~, the method comprising:

reading a certificate library server address from the chip card;

accessing a certificate library memory segment using the certificate library server address;

searching the certificate library memory segment for a digital certificate having an ~~entity~~ identifier that identifies said registration authority and followed by a digital certificate chain; and

traversing the digital certificate chain beginning with the digital certificate tagged by the registration authority identifier until a trusted root certificate is reached, whereby said user's relationship may be authenticated.

14. (currently amended) A method as recited in claim 13 wherein said chip card includes a user second cryptographic key and wherein said digital certificate includes a user first cryptographic key ~~further including storing a user private key and the certificate library address on the chip card~~.

15. (currently amended) A method as recited in claim 13 wherein the certificate library server is a Lightweight Directory Access Protocol (LDAP) server.

16. (currently amended) A method as recited in claim 13 further including storing additional digital certificates each having different registration authority identifiers at the certificate library memory segment.

17. (currently amended) A method as recited in claim 16 further including ~~associating~~ creating additional digital certificate chains using ~~with~~ the additional digital certificates, the certificate chains being stored in the memory segment and each certificate chain having its own trusted root.

18. (currently amended) A method as recited in claim 13 wherein searching the certificate library memory segment for a digital certificate further includes using specific parameters further specifying which portion of the certificate library memory segment contains a digital certificate issued by the registration authority.

19. (cancelled)

20. (cancelled)

Please add the following new claims:

21. (new) A method as recited in claim 1 wherein said issuing party is a registration authority, a certificate authority, a reliant party, a merchant or a service provider.

22. (new) A method as recited in claim 1 wherein said user private key on said chip card and a certificate store application on said chip card use about 2 kbytes of memory of said chip card.

23. (new) A method as recited in claim 9 further comprising:

prompting said user for a PIN, whereby said user is verified to be the owner of said chip card.

24. (new) A certificate library server for storing digital certificate chains of users, said certificate library server comprising:

a plurality of user-specific memory segments, each of said user-specific memory segments being accessible by an address contained in a chip card of one of said users;

a plurality of digital certificate chains issued to one of said users, said digital certificate chains included in one of said user-specific memory segments and each digital certificate chain being issued to said user by an issuer;

an issuer identifier associated with each digital certificate chain that identifies the issuer on whose behalf the digital certificate is provided in said certificate library server;

a user first cryptographic key included in each of said digital certificate chains, said user first cryptographic key having a corresponding user second cryptographic key being stored in the chip card of said user;

a set of user attributes included in each digital certificate chain providing information regarding the relationship between said user and the issuer associated with the digital certificate chain; and

a trusted root certificate for each digital certificate chain.

25. (new) A certificate library server as recited in claim 24 wherein said issuer is a registration authority, a certificate authority, a reliant party, a merchant or a service provider.

26. (new) A certificate library server as recited in claim 24 wherein said user first cryptographic key is a user public key and said user second cryptographic key is a user private key, whereby said keys implement an asymmetric cryptographic technique.

27. (new) A certificate library server as recited in claim 24 wherein said user first cryptographic key and said user second cryptographic key are the same, whereby said keys implement a symmetric cryptographic technique.

28. (new) A certificate library server as recited in claim 24 wherein the certificate library server is a Lightweight Directory Access Protocol (LDAP) server.

29. (new) A certificate store system for creating a digital certificate for a user, said certificate store system comprising:

a certificate authority arranged to create a user first cryptographic key and a corresponding user second cryptographic key, and arranged to create a digital certificate for said user that includes said user first cryptographic key;

a registration authority that requests creation of said digital certificate;

a certificate library server that stores said digital certificate in a memory location allotted to said user; and

a chip card that stores said user second cryptographic key, an address of said certificate library server, an identifier of said registration authority, and a software application that coordinates communication between said chip card and said certificate library server, whereby said digital certificate is stored remote from said chip card.

30. (new) A certificate store system as recited in claim 29 wherein said registration authority is said certificate authority, a reliant party, a merchant or a service provider.

31. (new) A certificate store system as recited in claim 29 wherein said user first cryptographic key is a user public key and said user second cryptographic key is a user private key, whereby said keys implement an asymmetric cryptographic technique.

32. (new) A certificate store system as recited in claim 29 wherein said user first cryptographic key and said user second cryptographic key are the same, whereby said keys implement a symmetric cryptographic technique.

a6

33. (new) A certificate store system as recited in claim 29 wherein the certificate library server is a Lightweight Directory Access Protocol (LDAP) server.

34. (new) A method as recited in claim 14 further comprising:

presenting an authentication challenge to said chip card to be encrypted by said user second cryptographic key;

receiving an encrypted response from said chip card; and

decrypting said encrypted response using said user first cryptographic key, whereby said chip card is authenticated.

35. (new) A method as recited in claim 34 further comprising:

prompting said user for a PIN, whereby said user is verified to be the owner of said chip card.

36. (new) A method as recited in claim 13 further comprising:

prompting said user for a PIN, whereby said user is verified to be the owner of said chip card.

37. (new) A chip card for authenticating a user's relationship with a registration authority, said chip card comprising:

a substrate; and

a computer chip mounted on said substrate, said computer chip including

an address of a certificate library server that includes a digital certificate created by a certificate authority whereby said digital certificate is stored remote from said chip card,

a software application arranged to coordinate communication between said chip card and said certificate library server using said address,

a user second cryptographic key created by said certificate authority, said user second cryptographic key corresponding to a user first cryptographic key also created by said certificate authority, said user first cryptographic key not being included in said chip card but being included in said digital certificate, and

an identifier that identifies said registration authority, whereby said software application assists with authenticating the user's relationship with a registration authority.

38. (new) A chip card as recited in claim 37 wherein said registration authority is said certificate authority, a reliant party, a merchant or a service provider.

39. (new) A chip card as recited in claim 37 wherein said user first cryptographic key is a user public key and said user second cryptographic key is a user private key, whereby said keys implement an asymmetric cryptographic technique.

40. (new) A chip card as recited in claim 37 wherein said user first cryptographic key and said user second cryptographic key are the same, whereby said keys implement a symmetric cryptographic technique.

41. (new) A chip card as recited in claim 37 wherein the certificate library server is a Lightweight Directory Access Protocol (LDAP) server.